

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-030138

(43)Date of publication of application : 31.01.2003

(51)Int.Cl. G06F 15/00
G06F 13/00
H04L 12/46
H04L 12/66

(21)Application number : 2001-211165

(71)Applicant : MITSUBISHI ELECTRIC CORP

(22)Date of filing : 11.07.2001

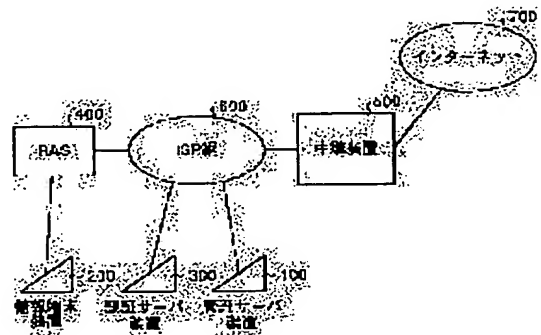
(72)Inventor : NAGASHIMA NORIMITSU
ATOZAWA SHINOBU

(54) INTERNET CONNECTION SYSTEM, MANAGING SEVER DEVICE, INTERNET CONNECTING METHOD, AND PROGRAM MAKING COMPUTER IMPLEMENT THE METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To provide safe Internet connection service for a user who does not have security knowledge without introducing implements and materials such as a firewall into individual users.

SOLUTION: An information terminal device 200 is connected to an ISP(Internet service provider) network 600 through a RAS(remote access server) 400. RAS 400 receives a connection request from the information terminal device 200 of a user and relays data to the ISP network 600. The ISP network 600 includes an authentication server device 300 which checks a user ID and a password and a managing server device 100 which manages information on contracting users. The managing server device 100 stores user information on application kinds, data directions, etc., that the user applied when making a contract.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J.P.)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-30138

(P 2003-30138A)

(43) 公開日 平成15年1月31日 (2003.1.31)

(51) Int. Cl. ⁷	識別記号	F I	テーマコード (参考)
G06F 15/00	310	G06F 15/00	310 D 5B085
13/00	351	13/00	351 Z 5B089
H04L 12/46		H04L 12/46	E 5K030
12/66		12/66	B 5K033

審査請求 未請求 請求項の数18 O L (全17頁)

(21) 出願番号 特願2001-211165 (P 2001-211165)

(22) 出願日 平成13年7月11日 (2001.7.11)

(71) 出願人 000006013

三菱電機株式会社

東京都千代田区丸の内二丁目2番3号

(72) 発明者 永嶋 規充

東京都千代田区丸の内二丁目2番3号 三

菱電機株式会社内

(72) 発明者 後沢 忍

東京都千代田区丸の内二丁目2番3号 三

菱電機株式会社内

(74) 代理人 100089118

弁理士 酒井 宏明

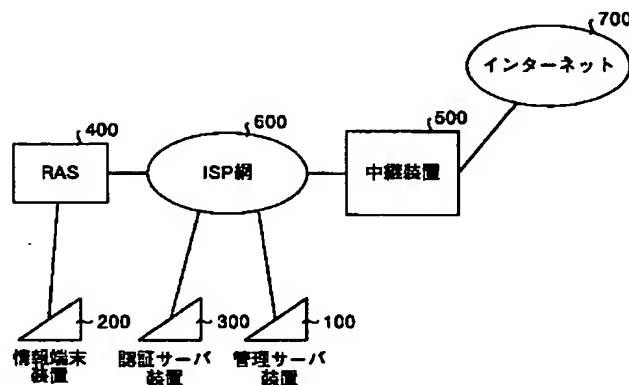
最終頁に続く

(54) 【発明の名称】 インターネット接続システム、管理サーバ装置、インターネット接続方法およびその方法をコンピュータに実行させるプログラム

(57) 【要約】

【課題】 ユーザ個々にファイアウォール等の機材を導入することなく、セキュリティ知識のないユーザに対して安全なインターネット接続サービスを提供すること。

【解決手段】 情報端末装置200は、RAS400を介してISP網600に接続される。RAS400は、ユーザの情報端末装置200からの接続要求を受け、データをISP網600に中継する。ISP網600には、ユーザID、パスワードをチェックする認証サーバ装置300、契約したユーザの情報を管理する管理サーバ装置100を含んで構成される。管理サーバ装置100には、ユーザが契約時に申請したアプリケーション種別やデータ方向等のユーザ情報が格納されている。



【特許請求の範囲】

【請求項 1】 ユーザの情報端末装置をインターネットに接続するためのインターネット接続システムにおいて、

前記ユーザが使用を許可するアプリケーションの種別に関するアプリケーション種別情報、および、前記ユーザが送受信を許可するデータの方向に関するデータ方向情報を登録する契約登録手段と、

前記ユーザに対してユーザ ID およびパスワードを発行する発行手段と、

前記ユーザが前記インターネットに接続する際に、当該ユーザの前記情報端末装置から前記ユーザ ID および前記パスワードを受信し、当該ユーザ ID および当該パスワードが前記発行手段によって前記ユーザに発行されたものであるか否かを認証する認証手段と、

前記認証手段によって認証された場合には、前記ユーザの前記情報端末装置に対して IP アドレスを割り当てる IP 割当手段と、

前記ユーザが送受信する前記データが前記契約登録手段によって登録された前記アプリケーション種別情報および前記データ方向情報に合致するか否かを判定する条件判定手段と、

を備え、前記条件判定手段によって合致すると判定された前記データについて送受信を許可することを特徴とするインターネット接続システム。

【請求項 2】 前記ユーザが前記インターネットの接続を切断した場合には、前記 IP 割当手段によって割り当てた前記 IP アドレスを無効にする IP アドレス無効手段をさらに備えたことを特徴とする請求項 1 に記載のインターネット接続システム。

【請求項 3】 前記契約登録手段によって登録された前記アプリケーション種別情報および前記データ方向情報を変更する契約変更手段、

をさらに備えたことを特徴とする請求項 1 または 2 に記載のインターネット接続システム。

【請求項 4】 前記条件判定手段によって合致しないと判定された場合には、前記データについて送受信する前記ユーザの前記情報端末装置に対して警告メッセージを送信する警告メッセージ送信手段、

をさらに備えたことを特徴とする請求項 1 ～ 3 のいずれか一つに記載のインターネット接続システム。

【請求項 5】 前記契約登録手段は、前記ユーザが使用を拒絶するアプリケーションの種別に関する拒絶アプリケーション種別情報、および、前記ユーザが送受信を拒絶するデータの方向に関する拒絶データ方向情報をさらに登録し、

前記条件判定手段は、前記ユーザが送受信する前記データが前記契約登録手段にて登録された前記拒絶アプリケーション種別情報および前記拒絶データ方向情報に合致するか否かを判定し、

前記条件判定手段によって前記拒絶アプリケーション種別情報および前記拒絶データ方向情報に合致すると判定した場合には、当該データを廃棄することを特徴とする請求項 1 ～ 4 のいずれか一つに記載のインターネット接続システム。

【請求項 6】 前記契約変更手段は、登録された前記アプリケーション種別情報と前記拒絶アプリケーション種別情報とを相互に変更可能にする種別変更手段と、

10 登録された前記データ方向情報と前記拒絶データ方向情報とを相互に変更可能にする方向変更手段と、

をさらに備えたことを特徴とする請求項 3 ～ 5 のいずれか一つに記載のインターネット接続システム。

【請求項 7】 ユーザの認証を行う認証サーバと、インターネットに接続された中継装置とを通信可能に接続して構成された、前記ユーザの情報端末装置を前記インターネットに接続するインターネット接続システムの管理サーバ装置において、

前記ユーザが使用を許可するアプリケーションの種別に関するアプリケーション種別情報、および、前記ユーザが送受信を許可するデータの方向に関するデータ方向情報を登録する契約登録手段と、

20 前記ユーザに対してユーザ ID およびパスワードを発行する発行手段と、

前記認証サーバにおいて前記ユーザ ID および前記パスワードが認証され、IP アドレスを割り当てられた前記ユーザに対して、当該 IP アドレスと、前記アプリケーション種別情報と、前記データ方向情報とを対応付けて格納するユーザ情報格納手段と、

30 前記ユーザ情報格納手段によって格納された当該 IP アドレスと、前記アプリケーション種別情報と、前記データ方向情報とを前記中継装置に対して送信するユーザ情報送信手段と、

を備え、前記中継装置において、前記ユーザが送受信する前記データが前記アプリケーション種別情報および前記データ方向情報に合致するか否かを判定し、合致すると判定された前記データについて送受信を許可することを特徴とする管理サーバ装置。

【請求項 8】 前記ユーザが前記インターネットの接続を切断した場合には、割り当てられた前記 IP アドレスを無効にする IP アドレス無効手段をさらに備えたことを特徴とする請求項 7 に記載の管理サーバ装置。

【請求項 9】 前記契約登録手段によって登録された前記アプリケーション種別情報および前記データ方向情報を変更する契約変更手段、

をさらに備えたことを特徴とする請求項 7 または 8 に記載の管理サーバ装置。

【請求項 10】 前記契約登録手段は、前記ユーザが使用を拒絶するアプリケーションの種別に関する拒絶アプリケーション種別情報、および、前記ユーザが送受信を

拒絶するデータの方向に関する拒絶データ方向情報をさらに登録し、

前記ユーザ情報格納手段は、前記ユーザの当該 IP アドレスと、前記拒絶アプリケーション種別情報と、前記拒絶データ方向情報とをさらに対応付けて格納し、

前記ユーザ情報送信手段は、前記ユーザの当該 IP アドレスと、前記拒絶アプリケーション種別情報と、前記拒絶データ方向情報とを前記中継装置に対してさらに送信し、

前記中継装置において、前記ユーザが送受信する前記データが前記拒絶アプリケーション種別情報および前記拒絶データ方向情報に合致するか否かを判定し、合致すると判定した場合には、当該データを廃棄することを特徴とする請求項 7～9 のいずれか一つに記載の管理サーバ装置。

【請求項 11】 前記契約変更手段は、登録された前記アプリケーション種別情報と前記拒絶アプリケーション種別情報とを相互に変更可能にする種別変更手段と、

登録された前記データ方向情報と前記拒絶データ方向情報とを相互に変更可能にする方向変更手段と、をさらに備えたことを特徴とする請求項 9 または 10 に記載の管理サーバ装置。

【請求項 12】 ユーザの情報端末装置をインターネットに接続するためのインターネット接続システムにおいて実行されるインターネット接続方法において、

前記ユーザが使用を許可するアプリケーションの種別に関するアプリケーション種別情報、および、前記ユーザが送受信を許可するデータの方向に関するデータ方向情報を登録する契約登録工程と、

前記ユーザに対してユーザ ID およびパスワードを発行する発行工程と、

前記ユーザが前記インターネットに接続する際に、当該ユーザの前記情報端末装置から前記ユーザ ID および前記パスワードを受信し、当該ユーザ ID および当該パスワードが前記発行工程によって前記ユーザに発行されたものであるか否かを認証する認証工程と、

前記認証工程によって認証された場合には、前記ユーザの前記情報端末装置に対して IP アドレスを割り当てる IP 割当工程と、

前記ユーザが送受信する前記データが前記契約登録工程によって登録されたアプリケーション種別情報および前記データ方向情報に合致するか否かを判定する条件判定工程と、

を含み、前記条件判定工程によって合致すると判定された前記データについて送受信を許可することを特徴とするインターネット接続方法。

【請求項 13】 前記ユーザが前記インターネットの接続を切断した場合には、前記 IP 割当工程によって割り当てた前記 IP アドレスを無効にする IP アドレス無効

工程をさらに含むことを特徴とする請求項 12 に記載のインターネット接続方法。

【請求項 14】 前記契約登録工程によって登録された前記アプリケーション種別情報および前記データ方向情報を変更する契約変更工程、

をさらに含むことを特徴とする請求項 12 または 13 に記載のインターネット接続方法。

【請求項 15】 前記条件判定工程によって合致しないと判定された場合には、前記データについて送受信する前記ユーザの前記情報端末装置に対して警告メッセージを送信する警告メッセージ送信工程、

をさらに含むことを特徴とする請求項 12～14 のいずれか一つに記載のインターネット接続方法。

【請求項 16】 前記契約登録工程は、前記ユーザが使用を拒絶するアプリケーションの種別に関する拒絶アプリケーション種別情報、および、前記ユーザが送受信を拒絶するデータの方向に関する拒絶データ方向情報をさらに登録し、

前記条件判定工程は、前記ユーザが送受信する前記データが前記契約登録工程にて登録された前記拒絶アプリケーション種別情報および前記拒絶データ方向情報に合致するか否かを判定し、

前記条件判定工程によって前記拒絶アプリケーション種別情報および前記拒絶データ方向情報に合致すると判定した場合には、当該データを廃棄することを特徴とする請求項 12～15 のいずれか一つに記載のインターネット接続方法。

【請求項 17】 前記契約変更工程は、登録された前記アプリケーション種別情報と前記拒絶アプリケーション種別情報とを相互に変更可能にする種別変更工程と、

登録された前記データ方向情報と前記拒絶データ方向情報とを相互に変更可能にする方向変更工程と、をさらに含むことを特徴とする請求項 14～16 のいずれか一つに記載のインターネット接続方法。

【請求項 18】 請求項 12～17 のいずれか一つに記載されたインターネット接続方法をコンピュータに実行させるプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 この発明は、ユーザの安全性を高めることができるインターネット接続システム、管理サーバ装置、インターネット接続方法およびその方法をコンピュータに実行させるプログラムに関するものである。

【0002】

【従来の技術】 インターネットの普及に伴い、会社や家庭からネットワークサービスを利用するユーザが増えている。また、近年、ADSL (Asynchronous Digital Subscriber Lin

e)、光ファイバなどの高速、広帯域ネットワーク技術の発展により、ユーザの利用形態はインターネットを利用する時だけ接続するダイヤルアップ接続から常時接続へと変化してきている。

【0003】ここで、インターネットを常時接続で使用する場合には、使用するアドレスが固定的になるため、接続の度に割り付けアドレスが変わるダイヤルアップ接続に比べ、悪意のあるユーザ（クラッカー）によるインターネットからの不正アクセスの危険性が高くなる問題がある。そのため、ユーザは、ファイアウォールなどの機器を導入し、不正アクセスに対処するケースが多く見られる。

【0004】図10は、文献「OPENDESIGN No. 14」第8頁（CQ出版社ISBN4-7898-1808-3）に記載されているファイアウォールが接続されたネットワーク構成図である。

【0005】図10において、組織ネットワーク63は、複数の組織内ネットワーク1、2、3（60、61、62）から構成される。組織ネットワーク63は、ルータ64を介してインターネット65に接続されている。ルータ64は、組織ネットワーク63からインターネット65への接続部分を1箇所に制限し、通過するデータのフィルタリングを行うことでファイアウォールとして動作し、組織ネットワーク63の安全性を保っている。

【0006】ここで、家庭からのインターネット接続における一般的なケースを一例として説明すると、端末67は、モデムを用いてインターネット接続サービスを提供するISP（Internet Service Provider）66にダイヤルアップして、インターネット65に接続する。

【0007】

【発明が解決しようとする課題】しかしながら、このようなケースでは、家庭の端末67には多くの場合フィルタリングを行うファイアウォールは存在せず、インターネット65とユーザの端末67との間の通信データはすべて許可されることになる。そのため、インターネット65から端末67への不正アクセスや、端末67からインターネット65への不用意なデータ流出の可能性がある。従って、上述した従来の方法では、不正アクセスを防止するためには、ユーザ個々にファイアウォールを導入する必要があるという問題がある。

【0008】また、ユーザが、導入したファイアウォールのルール設定を誤ることによりセキュリティが低下する恐れもあるため、ファイアウォールを導入する際にはネットワークやセキュリティに関する高度な知識がユーザに要求されるという問題がある。

【0009】この発明は上記に鑑みてなされたもので、ユーザ個々にファイアウォール等の機材を導入することなく、セキュリティ知識のないユーザに対して安全なイ

ンターネット接続サービスを提供することができるインターネット接続システム、管理サーバ装置、インターネット接続方法およびその方法をコンピュータに実行させるプログラムを得ることを目的とする。

【0010】

【課題を解決するための手段】上記目的を達成するため、この発明にかかるインターネット接続システムは、ユーザの情報端末装置をインターネットに接続するためのインターネット接続システムにおいて、前記ユーザが使用を許可するアプリケーションの種別に関するアプリケーション種別情報、および、前記ユーザが送受信を許可するデータの方向に関するデータ方向情報を登録する契約登録手段と、前記ユーザに対してユーザIDおよびパスワードを発行する発行手段と、前記ユーザが前記インターネットに接続する際に、当該ユーザの前記情報端末装置から前記ユーザIDおよび前記パスワードを受信し、当該ユーザIDおよび当該パスワードが前記発行手段によって前記ユーザに発行されたものであるか否かを認証する認証手段と、前記認証手段によって認証された場合には、前記ユーザの前記情報端末装置に対してIPアドレスを割り当てるIP割当手段と、前記ユーザが送受信する前記データが前記契約登録手段によって登録されたアプリケーション種別情報および前記データ方向情報に合致するか否かを判定する条件判定手段とを備え、前記条件判定手段によって合致すると判定された前記データについて送受信を許可することを特徴とする。

【0011】この発明によれば、ユーザが使用を許可するアプリケーションの種別に関するアプリケーション種別情報、および、ユーザが送受信を許可するデータの方向に関するデータ方向情報を登録し、ユーザに対してユーザIDおよびパスワードを発行し、ユーザが前記インターネットに接続する際に、ユーザの情報端末装置からユーザIDおよびパスワードを受信し、ユーザIDおよびパスワードがユーザに発行されたものであるか否かを認証し、認証された場合には、ユーザの情報端末装置に対してIPアドレスを割り当て、ユーザが送受信するデータが登録されたアプリケーション種別情報およびデータ方向情報に合致するか否かを判定し、合致すると判定されたデータについて送受信を許可するので、ユーザ個々にファイアウォール等の機材を導入することなく、セキュリティ知識のないユーザに対して安全なインターネット接続サービスを提供することができる。すなわち、ユーザは使用するアプリケーション種別とデータ方向をISP等に予め登録することにより、インターネットからユーザの情報端末装置への不正アクセスや、情報端末装置からインターネットへの不用意なデータ流出の可能性を低下させることができる。

【0012】つぎの発明にかかるインターネット接続システムは、上記の発明において、前記ユーザが前記インターネットの接続を切断した場合には、前記IP割当手

段によって割り当てた前記 IP アドレスを無効にする IP アドレス無効手段をさらに備えたことを特徴とする。

【0013】この発明によれば、ユーザがインターネットの接続を切断した場合には、IP 割当手段によって割り当てた前記 IP アドレスを無効にするので、ISP 等に設定されたユーザの情報を削除することができるようになる。

【0014】つぎの発明にかかるインターネット接続システムは、上記の発明において、前記契約登録手段によって登録された前記アプリケーション種別情報および前記データ方向情報を変更する契約変更手段をさらに備えたことを特徴とする。

【0015】この発明によれば、登録されたアプリケーション種別情報およびデータ方向情報を変更するので、ユーザは、使用を許可するアプリケーションやデータ方向を随時変更することができるようになる。

【0016】つぎの発明にかかるインターネット接続システムは、上記の発明において、前記条件判定手段によって合致しないと判定された場合には、前記データについて送受信する前記ユーザの前記情報端末装置に対して警告メッセージを送信する警告メッセージ送信手段をさらに備えたことを特徴とする。

【0017】この発明によれば、条件判定によって合致しないと判定された場合には、データについて送受信するユーザの情報端末装置に対して警告メッセージを送信するので、拒絶されたアプリケーションやデータ方向等をユーザに通知することができるようになる。

【0018】つぎの発明にかかるインターネット接続システムは、上記の発明において、前記契約登録手段は、前記ユーザが使用を拒絶するアプリケーションの種別に関する拒絶アプリケーション種別情報、および、前記ユーザが送受信を拒絶するデータの方向に関する拒絶データ方向情報をさらに登録し、前記条件判定手段は、前記ユーザが送受信する前記データが前記契約登録手段にて登録された前記拒絶アプリケーション種別情報および前記拒絶データ方向情報に合致するか否かを判定し、前記条件判定手段によって前記拒絶アプリケーション種別情報および前記拒絶データ方向情報に合致すると判定した場合には、当該データを廃棄することを特徴とする。

【0019】この発明によれば、ユーザが使用を拒絶するアプリケーションの種別に関する拒絶アプリケーション種別情報、および、ユーザが送受信を拒絶するデータの方向に関する拒絶データ方向情報をさらに登録し、ユーザが送受信するデータが登録された拒絶アプリケーション種別情報および拒絶データ方向情報に合致するか否かを判定し、条件判定によって拒絶アプリケーション種別情報および拒絶データ方向情報に合致すると判定した場合には、データを廃棄するので、ユーザは使用を拒絶するアプリケーションやデータの送受信を拒絶するデータ方向を予め ISP 等に登録することができるようにな

る。

【0020】つぎの発明にかかるインターネット接続システムは、上記の発明において、前記契約変更手段は、登録された前記アプリケーション種別情報と前記拒絶アプリケーション種別情報とを相互に変更可能にする種別変更手段と、登録された前記データ方向情報と前記拒絶データ方向情報とを相互に変更可能にする方向変更手段とをさらに備えたことを特徴とする。

【0021】この発明によれば、登録されたアプリケーション種別情報と拒絶アプリケーション種別情報とを相互に変更可能にし、登録されたデータ方向情報と拒絶データ方向情報とを相互に変更可能にするので、ユーザは、臨機応変に使用を許可または拒絶するアプリケーションやデータ方向を選択することができるようになる。

【0022】つぎの発明にかかるインターネット接続システムの管理サーバ装置は、ユーザの認証を行う認証サーバと、インターネットに接続された中継装置とを通信可能に接続して構成された、前記ユーザの情報端末装置を前記インターネットに接続するインターネット接続システムの管理サーバ装置において、前記ユーザが使用を許可するアプリケーションの種別に関するアプリケーション種別情報、および、前記ユーザが送受信を許可するデータの方向に関するデータ方向情報を登録する契約登録手段と、前記ユーザに対してユーザ ID およびパスワードを発行する発行手段と、前記認証サーバにおいて前記ユーザ ID および前記パスワードが認証され、IP アドレスを割り当てられた前記ユーザに対して、当該 IP アドレスと、前記アプリケーション種別情報と、前記データ方向情報とを対応付けて格納するユーザ情報格納手段と、前記ユーザ情報格納手段によって格納された当該 IP アドレスと、前記アプリケーション種別情報と、前記データ方向情報とを前記中継装置に対して送信するユーザ情報送信手段とを備え、前記中継装置において、前記ユーザが送受信する前記データが前記アプリケーション種別情報および前記データ方向情報に合致するか否かを判定し、合致すると判定された前記データについて送受信を許可することを特徴とする。

【0023】この発明によれば、ユーザが使用を許可するアプリケーションの種別に関するアプリケーション種別情報、および、ユーザが送受信を許可するデータの方向に関するデータ方向情報を登録し、ユーザに対してユーザ ID およびパスワードを発行し、認証サーバにおいてユーザ ID およびパスワードが認証され、IP アドレスを割り当てられたユーザに対して、IP アドレスと、アプリケーション種別情報と、データ方向情報とを対応付けて格納し、格納された IP アドレスと、アプリケーション種別情報と、データ方向情報とを中継装置に対して送信し、中継装置において、ユーザが送受信するデータがアプリケーション種別情報およびデータ方向情報に合致するか否かを判定し、合致すると判定されたデータ

について送受信を許可するので、ユーザ個々にファイアウォール等の機材を導入することなく、セキュリティ知識のないユーザに対して安全なインターネット接続サービスを提供することができる。すなわち、ユーザは使用するアプリケーション種別とデータ方向をISP等に予め登録することにより、インターネットからユーザの情報端末装置への不正アクセスや、情報端末装置からインターネットへの不用意なデータ流出の可能性を低下させることができる。

【0024】つぎの発明にかかるインターネット接続システムの管理サーバ装置は、上記の発明において、前記ユーザが前記インターネットの接続を切断した場合には、割り当てられた前記IPアドレスを無効にするIPアドレス無効手段をさらに備えたことを特徴とする。

【0025】この発明によれば、ユーザがインターネットの接続を切断した場合には、割り当てられた前記IPアドレスを無効にするので、ISP等に設定されたユーザの情報を削除することができるようになる。

【0026】つぎの発明にかかるインターネット接続システムの管理サーバ装置は、上記の発明において、前記契約登録手段によって登録されたアプリケーション種別情報および前記データ方向情報を変更する契約変更手段をさらに備えたことを特徴とする。

【0027】この発明によれば、登録されたアプリケーション種別情報および前記データ方向情報を変更するので、ユーザは、使用を許可するアプリケーションやデータ方向を随時変更することができるようになる。

【0028】つぎの発明にかかるインターネット接続システムの管理サーバ装置は、上記の発明において、前記契約登録手段は、前記ユーザが使用を拒絶するアプリケーションの種別に関する拒絶アプリケーション種別情報、および、前記ユーザが送受信を拒絶するデータの方向に関する拒絶データ方向情報をさらに登録し、前記ユーザ情報格納手段は、前記ユーザの当該IPアドレスと、前記拒絶アプリケーション種別情報と、前記拒絶データ方向情報とをさらに対応付けて格納し、前記ユーザ情報送信手段は、前記ユーザの当該IPアドレスと、前記拒絶アプリケーション種別情報と、前記拒絶データ方向情報とを前記中継装置に対してさらに送信し、前記中継装置において、前記ユーザが送受信する前記データが前記拒絶アプリケーション種別情報および前記拒絶データ方向情報に合致するか否かを判定し、合致すると判定した場合には、当該データを廃棄することを特徴とする。

【0029】この発明によれば、ユーザが使用を拒絶するアプリケーションの種別に関する拒絶アプリケーション種別情報、および、ユーザが送受信を拒絶するデータの方向に関する拒絶データ方向情報をさらに登録し、ユーザが送受信するデータが登録された拒絶アプリケーション種別情報および拒絶データ方向情報に合致するか否

かを判定し、条件判定によって拒絶アプリケーション種別情報および拒絶データ方向情報に合致すると判定した場合には、データを廃棄するので、ユーザは使用を拒絶するアプリケーションやデータの送受信を拒絶するデータ方向を予めISP等に登録することができるようになる。

【0030】つぎの発明にかかるインターネット接続システムの管理サーバ装置は、上記の発明において、前記契約変更手段は、登録された前記アプリケーション種別情報と前記拒絶アプリケーション種別情報とを相互に変更可能にする種別変更手段と、登録された前記データ方向情報と前記拒絶データ方向情報とを相互に変更可能にする方向変更手段とをさらに備えたことを特徴とする。

【0031】この発明によれば、登録されたアプリケーション種別情報と拒絶アプリケーション種別情報とを相互に変更可能にし、登録されたデータ方向情報と拒絶データ方向情報とを相互に変更可能にするので、ユーザは、臨機応変に使用を許可または拒絶するアプリケーションやデータ方向を選択することができるようになる。

【0032】上記目的を達成するため、この発明にかかるインターネット接続方法は、ユーザの情報端末装置をインターネットに接続するためのインターネット接続システムを用いて実行されるインターネット接続方法において、前記ユーザが使用を許可するアプリケーションの種別に関するアプリケーション種別情報、および、前記ユーザが送受信を許可するデータの方向に関するデータ方向情報を登録する契約登録工程と、前記ユーザに対してユーザIDおよびパスワードを発行する発行工程と、前記ユーザが前記インターネットに接続する際に、当該ユーザの前記情報端末装置から前記ユーザIDおよび前記パスワードを受信し、当該ユーザIDおよび当該パスワードが前記発行工程によって前記ユーザに発行されたものであるか否かを認証する認証工程と、前記認証工程によって認証された場合には、前記ユーザの前記情報端末装置に対してIPアドレスを割り当てるIP割当工程と、前記ユーザが送受信する前記データが前記契約登録工程によって登録されたアプリケーション種別情報および前記データ方向情報に合致するか否かを判定する条件判定工程とを含み、前記条件判定工程によって合致すると判定された前記データについて送受信を許可することを特徴とする。

【0033】この発明によれば、ユーザが使用を許可するアプリケーションの種別に関するアプリケーション種別情報、および、ユーザが送受信を許可するデータの方向に関するデータ方向情報を登録し、ユーザに対してユーザIDおよびパスワードを発行し、ユーザが前記インターネットに接続する際に、ユーザの情報端末装置からユーザIDおよびパスワードを受信し、ユーザIDおよびパスワードがユーザに発行されたものであるか否かを認証し、認証された場合には、ユーザの情報端末装置に

対して IP アドレスを割り当て、ユーザが送受信するデータが登録されたアプリケーション種別情報およびデータ方向情報に合致するか否かを判定し、合致すると判定されたデータについて送受信を許可するので、ユーザ個々にファイアウォール等の機材を導入することなく、セキュリティ知識のないユーザに対して安全なインターネット接続サービスを提供することができる。すなわち、ユーザは使用するアプリケーション種別とデータ方向を ISP 等に予め登録することにより、インターネットからユーザの情報端末装置への不正アクセスや、情報端末装置からインターネットへの不要なデータ流出の可能性を低下させることができる。

【0034】つぎの発明にかかるインターネット接続方法は、上記の発明において、前記ユーザが前記インターネットの接続を切断した場合には、前記 IP 割当工程によって割り当てた前記 IP アドレスを無効にする IP アドレス無効工程をさらに含むことを特徴とする。

【0035】この発明によれば、ユーザがインターネットの接続を切断した場合には、IP 割当工程によって割り当てた前記 IP アドレスを無効にするので、ISP 等に設定されたユーザの情報を削除することができるようになる。

【0036】つぎの発明にかかるインターネット接続方法は、上記の発明において、前記契約登録工程によって登録された前記アプリケーション種別情報および前記データ方向情報を変更する契約変更工程をさらに含むことを特徴とする。

【0037】この発明によれば、登録されたアプリケーション種別情報および前記データ方向情報を変更するので、ユーザは、使用を許可するアプリケーションやデータ方向を随時変更することができるようになる。

【0038】つぎの発明にかかるインターネット接続方法は、上記の発明において、前記条件判定工程によって合致しないと判定された場合には、前記データについて送受信する前記ユーザの前記情報端末装置に対して警告メッセージを送信する警告メッセージ送信工程をさらに含むことを特徴とする。

【0039】この発明によれば、条件判定によって合致しないと判定された場合には、データについて送受信するユーザの情報端末装置に対して警告メッセージを送信するので、拒絶されたアプリケーションやデータ方向等をユーザに通知することができるようになる。

【0040】つぎの発明にかかるインターネット接続方法は、上記の発明において、前記契約登録工程は、前記ユーザが使用を拒絶するアプリケーションの種別に関する拒絶アプリケーション種別情報、および、前記ユーザが送受信を拒絶するデータの方向に関する拒絶データ方向情報をさらに登録し、前記条件判定工程は、前記ユーザが送受信する前記データが前記契約登録工程にて登録された前記拒絶アプリケーション種別情報および前記拒

絶データ方向情報に合致するか否かを判定し、前記条件判定工程によって前記拒絶アプリケーション種別情報および前記拒絶データ方向情報に合致すると判定した場合には、当該データを廃棄することを特徴とする。

【0041】この発明によれば、ユーザが使用を拒絶するアプリケーションの種別に関する拒絶アプリケーション種別情報、および、ユーザが送受信を拒絶するデータの方向に関する拒絶データ方向情報をさらに登録し、ユーザが送受信するデータが登録された拒絶アプリケーション種別情報および拒絶データ方向情報に合致するか否かを判定し、条件判定によって拒絶アプリケーション種別情報および拒絶データ方向情報に合致すると判定した場合には、データを廃棄するので、ユーザは使用を拒絶するアプリケーションやデータの送受信を拒絶するデータ方向を予め ISP 等に登録することができるようになる。

【0042】つぎの発明にかかるインターネット接続方法は、上記の発明において、前記契約変更工程は、登録された前記アプリケーション種別情報と前記拒絶アプリケーション種別情報とを相互に変更可能にする種別変更工程と、登録された前記データ方向情報と前記拒絶データ方向情報とを相互に変更可能にする方向変更工程とをさらに含むことを特徴とする。

【0043】この発明によれば、登録されたアプリケーション種別情報と拒絶アプリケーション種別情報とを相互に変更可能にし、登録されたデータ方向情報と拒絶データ方向情報とを相互に変更可能にするので、ユーザは、臨機応変に使用を許可または拒絶するアプリケーションやデータ方向を選択することができるようになる。

【0044】つぎの発明にかかるプログラムは、上記の発明のいずれか一つに記載されたインターネット接続方法をコンピュータに実行させるプログラムであり、そのプログラムが機械読み取り可能となり、これによって、上記の発明のいずれか一つの動作をコンピュータによって実行することができる。

【0045】

【発明の実施の形態】以下に添付図面を参照して、この発明にかかるインターネット接続システム、管理サーバ装置、インターネット接続方法およびその方法をコンピュータに実行させるプログラムの好適な実施の形態を詳細に説明する。

【0046】実施の形態 1. 図 1 は、この発明の実施の形態 1 であるインターネット接続システムのネットワーク構成を示すブロック図である。図 1 において、情報端末装置 200 は、RAS (Remote Access Server) 400 を介して ISP 網 600 に接続される。RAS 400 は、ユーザの情報端末装置 200 からの接続要求を受け、データを ISP 網 600 に中継する。ISP 網 600 には、ユーザ ID、パスワードをチェックする認証サーバ装置 300、契約したユーザの

情報を管理する管理サーバ装置 100 を含んで構成される。管理サーバ装置 100 には、ユーザが契約時に申請したアプリケーション種別やデータ方向等のユーザ情報が格納されている。ISP 網 600 は、中継装置 500 を経由してインターネット 700 に接続されている。ここで、本実施の形態では、RAS や中継装置等のようにデータを中継、転送する機器をネットワーク機器と称する。

【0047】図 2 は、本発明が適用される管理サーバ装置 100 の構成の一例を示すブロック図であり、該構成のうち本発明に関係する部分のみを概念的に示している。図 2 において管理サーバ装置 100 は、概略的に、管理サーバ装置 100 の全体を統括的に制御する CPU 等の制御部 102、通信回線等に接続されるルータ等の通信装置（図示せず）に接続される通信制御インターフェース部 104、および、各種のデータベース（ユーザ情報データベース 106a）を格納する記憶部 106 を備えて構成されており、これら各部は任意の通信路を介して通信可能に接続されている。さらに、このサーバ装置は、ルータ等の通信装置および専用線等の有線または無線の通信回線を介して、ISP 網 600 に通信可能に接続されている。

【0048】図 2 の記憶部 106 に格納される各種のデータベース（ユーザ情報データベース 106a）は、固定ディスク装置等のストレージ手段であり、各種処理やウェブサイト提供に用いる各種のプログラムやテーブルやファイルやデータベースやウェブページ用ファイル等を格納する。

【0049】これら記憶部 106 の各構成要素のうち、ユーザ情報データベース 106a は、ユーザに関する情報（ユーザ情報）を格納するユーザ情報格納手段であり、認証サーバにおいてユーザ ID およびパスワードが認証され、IP アドレスを割り当てられたユーザに対して、IP アドレスと、アプリケーション種別情報と、データ方向情報とを対応付けて格納するユーザ情報格納手段である。ここで、図 7 は、ユーザ情報データベース 106a に格納されるユーザ情報の一例を示す図である。

【0050】このユーザ情報データベース 106a に格納される情報は、図 7 に示すように、各ユーザを一意に識別するためのユーザ名（ユーザ ID）40、ユーザに割り当てられる割り当て IP アドレス 41、ユーザが使用するアプリケーション種別に関するアプリケーション種別情報 42、ユーザが送受信するデータの方向に関するデータ方向情報 43、ユーザがアプリケーションの使用やデータ送受信を許可するかまたは拒絶するかを指定するフラグ 44 等から構成される。

【0051】また、その他の情報として、管理サーバ装置 100 の記憶部 106 には、ウェブサイトを情報端末装置 200 に提供するための各種の Web データや CGI プログラム等が記録されている。

【0052】この Web データとしては、後述する各種の Web ページを表示するためのデータ等があり、これらデータは、例えば、HTML や XML にて記述されたテキストファイルとして形成されている。また、これらの Web データを作成するための部品用のファイルや作業用のファイルやその他一時的なファイル等も記憶部 106 に記憶される。

【0053】この他、必要に応じて、情報端末装置 200 に送信するための音声データを WAVE 形式や A I F F 形式の如き音声ファイルで格納したり、静止画や動画を J P E G 形式や M P E G 2 形式の如き画像ファイルで格納したりすることができる。

【0054】また、図 2 において、通信制御インターフェース部 104 は、管理サーバ装置 100 と ISP 網 600（またはルータ等の通信装置）との間における通信制御を行う。すなわち、通信制御インターフェース部 104 は、他の端末と通信回線を介してデータを通信する機能を有する。

【0055】また、図 2 において、制御部 102 は、OS (Operating System) 等の制御プログラム、各種の処理手順等を規定したプログラム、および所要データを格納するための内部メモリを有し、これらのプログラム等により、種々の処理を実行するための情報処理を行う。制御部 102 は、機能概念的に、契約登録部 102a、契約変更部 102b、ID・パスワード発行部 102c、IP アドレス無効部 102d、および、ユーザ情報送信部 102e を備えて構成されている。

【0056】このうち、契約登録部 102a は、ユーザが使用を許可するアプリケーションの種別に関するアプリケーション種別情報、および、ユーザが送受信を許可するデータの方向に関するデータ方向情報を登録する契約登録手段である。また、契約変更部 102b は、契約登録手段によって登録されたアプリケーション種別情報およびデータ方向情報を変更する契約変更手段である。また、ID・パスワード発行部 102c は、ユーザに対してユーザ ID およびパスワードを発行する発行手段である。

【0057】また、IP アドレス無効部 102d は、ユーザがインターネットの接続を切断した場合には、割り当てた IP アドレスを無効にする IP アドレス無効手段である。また、ユーザ情報送信部 102e は、ユーザ情報格納手段によって格納された IP アドレスと、アプリケーション種別情報と、データ方向情報とを中継装置に対して送信するユーザ情報送信手段である。なお、これら各部によって行なわれる処理の詳細については、後述する。

【0058】また、図 3 は、本発明が適用される認証サーバ装置 300 の構成の一例を示すブロック図であり、該構成のうち本発明に関係する部分のみを概念的に示し

ている。図 3 において認証サーバ装置 300 は、概略的に、認証サーバ装置 300 の全体を統括的に制御する CPU 等の制御部 302、通信回線等に接続されるルータ等の通信装置（図示せず）に接続される通信制御インターフェース部 304、および、各種のデータベース（ユーザ認証情報データベース 306a および IP アドレス情報データベース 306b）を格納する記憶部 306 を備えて構成されており、これら各部は任意の通信路を介して通信可能に接続されている。さらに、このサーバ装置は、ルータ等の通信装置および専用線等の有線または無線の通信回線を介して、ISP 網 600 に通信可能に接続されている。

【0059】図 3 の記憶部 306 に格納される各種のデータベース（ユーザ認証情報データベース 306a および IP アドレス情報データベース 306b）は、固定ディスク装置等のストレージ手段であり、各種処理やウェブサイト提供に用いる各種のプログラムやテーブルやファイルやデータベースやウェブページ用ファイル等を格納する。

【0060】これら記憶部 306 の各構成要素のうち、ユーザ認証情報データベース 306a は、ユーザ認証に関する情報（ユーザ認証情報）を格納するユーザ認証情報格納手段である。このユーザ認証情報データベース 306a に格納される情報は、各ユーザを一意に識別するためのユーザ ID、および、パスワードから構成される。

【0061】また、IP アドレス情報データベース 306b は、システム内で利用可能な IP アドレスの利用状況を管理する IP アドレス情報を格納する IP アドレス情報格納手段である。この IP アドレス情報データベース 306b に格納される情報は、IP アドレスと、当該 IP アドレスを使用しているユーザのユーザ ID から構成される。

【0062】また、図 3 において、通信制御インターフェース部 304 は、認証サーバ装置 300 と ISP 網 600（またはルータ等の通信装置）との間における通信制御を行う。すなわち、通信制御インターフェース部 304 は、他の端末と通信回線を介してデータを通信する機能を有する。

【0063】また、図 3 において、制御部 302 は、OS (Operating System) 等の制御プログラム、各種の処理手順等を規定したプログラム、および所要データを格納するための内部メモリを有し、これらのプログラム等により、種々の処理を実行するための情報処理を行う。制御部 302 は、機能概念的に、ユーザ認証部 302a、および、IP アドレス割当部 302b を備えて構成されている。

【0064】このうち、ユーザ認証部 302a は、ユーザがインターネットに接続する際に、ユーザの情報端末装置からユーザ ID およびパスワードを受信し、ユーザ

ID およびパスワードが発行手段によってユーザに発行されたものであるか否かを認証する認証手段である。また、IP アドレス割当部 302b は、認証手段によって認証された場合には、ユーザの情報端末装置に対して IP アドレスを割り当てる IP 割当手段である。なお、これら各部によって行なわれる処理の詳細については、後述する。

【0065】また、図 4 は、本発明が適用される中継装置 500 の構成の一例を示すブロック図であり、該構成のうち本発明に関係する部分のみを概念的に示している。図 4 において中継装置 500 は、概略的に、中継装置 500 の全体を統括的に制御する CPU 等の制御部 502、通信回線等に接続されるルータ等の通信装置（図示せず）に接続される通信制御インターフェース部 504、および、各種のデータベース（ユーザ情報データベース 506a）を格納する記憶部 506 を備えて構成されており、これら各部は任意の通信路を介して通信可能に接続されている。さらに、このサーバ装置は、ルータ等の通信装置および専用線等の有線または無線の通信回線を介して、ISP 網 600 またはインターネット 700 に通信可能に接続されている。

【0066】図 4 の記憶部 506 に格納される各種のデータベース（ユーザ情報データベース 506a）は、固定ディスク装置等のストレージ手段であり、各種処理やウェブサイト提供に用いる各種のプログラムやテーブルやファイルやデータベースやウェブページ用ファイル等を格納する。

【0067】記憶部 506 の各構成要素のうち、ユーザ情報データベース 506a は、管理サーバ装置 100 から送信されたユーザ情報格納手段であり、ユーザ情報データベース 106a と同一の内容が格納されている。

【0068】また、図 4 において、通信制御インターフェース部 504 は、中継装置 500 と ISP 網 600 またはインターネット 700（またはルータ等の通信装置）との間における通信制御を行う。すなわち、通信制御インターフェース部 504 は、他の端末と通信回線を介してデータを通信する機能を有する。

【0069】また、図 4 において、制御部 502 は、OS (Operating System) 等の制御プログラム、各種の処理手順等を規定したプログラム、および所要データを格納するための内部メモリを有し、これらのプログラム等により、種々の処理を実行するための情報処理を行う。制御部 502 は、機能概念的に、データ受信部 502a、ユーザ特定部 502b、条件判定部 502c、データ送信部 502d、警告メッセージ送信部 502e、および、ユーザ情報更新部 502f を備えて構成されている。

【0070】このうち、データ受信部 502a は、ユーザが送受信するデータを受信するデータ受信手段である。また、ユーザ特定部 502b は、送受信するデータ

10

20

30

40

50

の宛先または送信元の IP アドレスから送受信するユーザを特定するユーザ特定手段である。また、条件判定部 502c は、ユーザが送受信するデータが契約登録手段によって登録されたアプリケーション種別情報およびデータ方向情報に合致するか否かを判定する条件判定手段である。

【0071】また、データ送信部 502d は、条件判定手段によって許可された条件に合致する（または拒絶された条件に合致しない）と判定されたデータについてデータを送信するデータ送信手段である。また、警告メッセージ送信部 502e は、条件判定手段によって許可された条件に合致しない（または拒絶された条件に合致する）と判定された場合には、データについて送受信するユーザの情報端末装置に対して警告メッセージを送信する警告メッセージ送信手段である。また、ユーザ情報更新部 502f は、管理サーバ装置 100 から受信したユーザ情報に基づいてユーザ情報データベース 506a を更新するユーザ情報更新手段である。なお、これら各部によって行なわれる処理の詳細については、後述する。

【0072】また、図 5 は、本発明が適用される情報端末装置 200 の構成の一例を示すブロック図であり、該構成のうち本発明に関係する部分のみを概念的に示している。この図 5 に示すように、情報端末装置 200 は、概略的には、制御部 210、ROM 220、HD 230、RAM 240、入力装置 250、出力装置 260、入出力制御 IF 270、および、通信制御 IF 280 を備えて構成されており、これら各部がバスを介してデータ通信可能に接続されている。

【0073】この情報端末装置 200 の制御部 210 は、Web ブラウザ 211 および電子メール 212 を備えて構成されている。このうち、Web ブラウザ 211 は、基本的には、Web データを解釈して、後述するモニタ 261 に表示させる表示制御（ブラウズ処理）を行うものである。また、電子メール 212 は、所定の通信規約（例えば、SMTP（Simple Mail Transfer Protocol））に従って、電子メールの送受信を行う。

【0074】また、入力装置 250 としては、キーボード、マウス、および、マイク等を用いることができる。また、後述するモニタ 261 も、マウスと協働してポインティングデバイス機能を実現する。

【0075】また、出力装置 260 としては、モニタ（家庭用テレビを含む）261、および、プリンタ 262 が設けられている。この他、出力装置 260 としては、スピーカ等を用いることができる。出力装置 260 は、通信制御 IF 280 を介して受信された情報を出力する出力手段である。

【0076】また、通信制御 IF 280 は、情報端末装置 200 とネットワーク（またはルータ等の通信装置）との間における通信制御を行う。この通信制御 IF 28

0 は、管理サーバ装置 100 から送信された情報を受信する受信手段である。

【0077】このように構成された情報端末装置 200 は、モデム、TA、ルータ等の通信装置と電話回線を介して、あるいは、専用線を介して、ネットワークに接続されており、所定の通信規約（たとえば、TCP/IP インターネットプロトコル）に従って RAS 400 にアクセスすることができる。

【0078】次に、このように構成された本実施の形態における本システムの処理の一例について、以下に図 6～図 8 を参照して詳細に説明する。図 6 は、本実施形態における本システムを用いて、ユーザがインターネットサービスを利用する際の動作の一例を示すフローチャートである。

【0079】まず、ユーザは、インターネットサービスを利用するにあたり、ISP 等のユーザに対してインターネット接続サービスを提供するインターネット接続システムと契約を行う。すなわち、ユーザは、契約時に住所、氏名、電話番号を通知すると共に、例えば、電子メールやホームページ参照等のユーザが使用するアプリケーション種別、ユーザが送受信するデータ方向、および、このアプリケーション種別やデータ方向を許可するか拒絶するかを指定するためのフラグからなるユーザ情報を ISP に通知する（ステップ SA-1）。ISP は、管理サーバ装置 100 の契約登録部 102a の処理により、通知されたこれらの情報をユーザ情報データベース 106a に登録する。

【0080】ここで、図 7 は、ユーザ名（ユーザ ID）として neko を指定し、アプリケーション種別として E-mail を指定し、データ方向としてユーザからインターネットを指定し、フラグとして許可を指定し、また、アプリケーション種別としてホームページ閲覧を指定し、データ方向としてユーザからインターネットを指定し、フラグとして拒絶をユーザ情報に指定した場合の管理サーバ装置 100 のユーザ情報データベース 106a に格納される情報の一例である。

【0081】なお、ISP が、インターネット初心者ユーザに対して、お薦めメニューとしてアプリケーション種別（E-mail、WWW 等）、データ方向（ユーザからインターネットへ、または、インターネットからユーザへ）、フラグ（許可、拒絶）を表示するメニュー画面を用意し、ユーザの情報端末装置 200 に表示させてもよい。これにより、初心者ユーザも安心して本システムを利用することができるようになる。

【0082】ついで、ISP は、管理サーバ装置 100 の ID・パスワード発行部 102c の処理により、ユーザに対してインターネット接続で使用するユーザ ID、パスワードを発行し、認証サーバ装置 300 のユーザ認証情報データベース 306a にこれらのユーザ認証情報を登録する（ステップ SA-2）。

【0083】 19 ついで、ユーザは、インターネットサービス利用時にRAS400に接続し、ID、パスワードを通知する(ステップSA-3)。

【0084】 ついで、認証サーバ装置300は、ユーザ認証部302aの処理により、通知されたID、パスワードをユーザ認証情報データベース306aにアクセスして検証し、不正な場合は接続を遮断する。一方、正しい場合には、IPアドレス割当部302bの処理により、IPアドレス情報データベース306bの中に保持している使用可能なIPアドレスの中から1つを選び、このユーザに割り当てる(ステップSA-4)。

【0085】 認証サーバ装置300は、ユーザに割り当てたIPアドレスを管理サーバ装置100に対して通知し、管理サーバ装置100では、該通知された割り当てIPアドレスをユーザ情報データベース106aに登録する。

【0086】 ついで、管理サーバ装置100は、ユーザ情報送信部102eの処理により、ユーザ情報データベース106aに格納されたユーザ情報を中継装置500に対して配送する。

【0087】 ついで、ユーザがデータをISPに対して送信すると(ステップSA-5)、中継装置が該データを受信し、図8で示される処理が実行される。図8は、データ受信時の中継装置500の動作の一例を示すフローチャートである。

【0088】 ここで、中継装置500におけるデータ受信は、ユーザがインターネットに対して送信したデータ、または、インターネット側から受信したデータの両方のデータに対して行われる。

【0089】 まず、中継装置500は、データ受信部502aの処理により、データを受信すると(ステップSB-1)、ユーザ特定部502bの処理により、受信データの送信元あるいは宛先アドレスからユーザを特定する(ステップSB-2)。

【0090】 次に、中継装置500は、条件判定部502cの処理により、特定したユーザについてユーザ情報データベース506aを参照して、取得したアプリケーション種別、通信方向、および、フラグの各条件が、受信したデータと合致するかをチェックする(ステップSB-3)。

【0091】 ここで、中継装置500は、条件が一致する場合(すなわち、許可された条件に合致するか、または拒絶された条件に合致しない場合)には、データ送信部502dの処理によりデータを送信し(ステップSB-4)、一方、条件が一致しない場合(すなわち、許可された条件に合致しないか、または拒絶された条件に合致する場合)には、警告メッセージ送信部502eの処理により、データを廃棄し、予め契約登録した以外のデータを受信したことを警告メッセージとしてユーザに通知する(ステップSB-5)。

【0092】 上記の例のように、ユーザが指定したアプリケーション条件に一致したものを送信し、その他をすべて廃棄してもよく、また、条件に一致したものを廃棄し、その他のデータを送信してもよい。

【0093】 再び、図6に戻り、中継装置500の処理により、予めユーザが契約登録した条件に合致するデータのみが送受信される(ステップSA-6～ステップSA-8)。

【0094】 最後に、ユーザがインターネット接続を切断した場合には、RAS400がこれを検知し、管理サーバ装置100に通知する。

【0095】 管理サーバ装置100は、IPアドレス無効部102dの処理により、ユーザ情報データベース106aに格納されたユーザ情報内のIPアドレスを無効にし、また、ユーザ情報送信部102eの処理により、その旨を中継装置500に通知する。中継装置500では、ユーザ情報更新部502fの処理により、対応するユーザ情報データベース506aのユーザ情報が削除される(ステップSA-9)。

20 【0096】 以上により、ユーザ側で個々にセキュリティ機器を導入することなく、安全なインターネットサービスを提供できる。また、典型的なメニューを用意することでセキュリティ知識のないユーザや初心者ユーザも安全にインターネットを利用することが可能となる。

【0097】 本実施の形態では、ユーザがRASに接続する構成を示したが、RASの代わりにADSLモデムを用いるような常時接続形態も可能である。

【0098】 実施の形態2。 つぎに、この発明の実施の形態2について説明する。本実施の形態2では、新たなアプリケーションとしてネットワークゲームを行う場合のように、契約登録したアプリケーション種別をユーザが変更する場合の動作を説明する。図9は、実施の形態2である本システムの動作の一例を示すフローチャートである。なお、ネットワーク構成および各装置の構成は、実施の形態1において図1～図5で示したものと同様である。

【0099】 まず、ユーザは、ユーザID、パスワードを入力して(ステップSC-1)、情報端末装置200からISP網600に送信すると(ステップSC-2)、認証サーバ装置300は、ユーザ認証部302aの処理により、ユーザID、パスワードをチェックする(ステップSC-3)。

【0100】 そして、チェックがOKであれば、管理サーバ装置100は、契約変更部102bの処理により、ユーザ情報データベース106aに格納されたユーザ情報のアプリケーション種別情報、データ方向情報、または、フラグの変更をユーザに許容する(ステップSC-4)。

50 【0101】 これにより、ユーザは、登録されたアプリケーション種別情報およびデータ方向情報を変更するこ

とができ、ユーザは、使用を許可するアプリケーションやデータ方向を随時変更することができるようになる。

【0102】また、契約変更部102bは、フラグをユーザに変更させることにより、登録されたアプリケーション種別情報と拒絶アプリケーション種別情報とを相互に変更可能にし、また、登録されたデータ方向情報と拒絶データ方向情報とを相互に変更可能にすることもできるので、ユーザは、使用を許可または拒絶するアプリケーションやデータ方向を臨機応変に選択することができるようになる。

【0103】ついで、管理サーバ装置100は、契約変更部102bの処理により、ユーザの変更結果によりユーザ情報データベース106aを更新した後、ユーザ情報送信部102eの処理により、該ユーザ情報を中継装置500に対して配信する(ステップSC-5)。

【0104】一方、ステップSC-3においてチェック結果がNGの場合は、管理サーバ装置100は、エラー情報をユーザの情報端末装置200に表示し(ステップSC-6)、処理を終了する。以上により、ユーザは申請した使用するアプリケーションを安全に変更できる。また、これにより、新たなアプリケーションを使用した場合にも容易に対応できる。

【0105】さて、これまで本発明の実施の形態について説明したが、本発明は、上述した実施の形態以外にも、上記特許請求の範囲に記載した技術的思想の範囲内において種々の異なる実施の形態にて実施されてよいものである。

【0106】また、実施の形態において説明した各処理のうち、自動的に行なわれるものとして説明した処理の全部または一部を手動的に行うこともでき、あるいは、手動的に行なわれるものとして説明した処理の全部または一部を公知の方法で自動的に行うこともできる。この他、上記文書中や図面中で示した処理手順、制御手順、具体的名称、各種の登録データや検索条件等のパラメータを含む情報、画面例、データベース構成については、特記する場合を除いて任意に変更することができる。

【0107】また、管理サーバ装置100に関して、図示の各構成要素は機能概念的なものであり、必ずしも物理的に図示の如く構成されていることを要しない。例えば、管理サーバ装置100、認証サーバ装置300、RAS400、中継装置500の各サーバ等が備える処理機能、特に制御部にて行なわれる各処理機能については、その全部または任意の一部を、CPU(Central Processing Unit)および当該CPUにて解釈実行されるプログラムにて実現することができ、あるいは、ワイヤードロジックによるハードウェアとして実現することも可能である。

【0108】なお、プログラムは、後述する記録媒体に記録されており、必要に応じて管理サーバ装置100、認証サーバ装置300、RAS400、中継装置500

に機械的に読み取られる。

【0109】また、管理サーバ装置100、認証サーバ装置300、RAS400、中継装置500は、さらなる構成要素として、マウス等の各種ポインティングデバイスやキーボードやイメージスキャナやデジタイザ等から成る入力装置(図示せず)、入力データのモニタに用いる表示装置(図示せず)、システムクロックを発生させるクロック発生部(図示せず)、および、各種処理結果その他のデータを出力するプリンタ等の出力装置(図示せず)を備えてもよい。

【0110】また、入力装置、表示装置および出力装置は、それぞれ入出力インターフェースを介して制御部に接続されてもよい。

【0111】記憶部に格納される各種のデータベースは、RAM、ROM等のメモリ装置、ハードディスク等の固定ディスク装置、フレキシブルディスク、光ディスク等のストレージ手段であり、各種処理やウェブサイト提供に用いる各種のプログラムやテーブルやファイルやデータベースやウェブページ用ファイル等を格納する。

【0112】また、管理サーバ装置100、認証サーバ装置300、RAS400、中継装置500は、既知のパーソナルコンピュータ、ワークステーション等の情報処理端末等の情報処理装置にプリンタやモニタやイメージスキャナ等の周辺装置を接続し、該情報処理装置に本発明の方法を実現させるソフトウェア(プログラム、データ等を含む)を実装することにより実現してもよい。

【0113】さらに、管理サーバ装置100、認証サーバ装置300、RAS400、中継装置500の分散・統合の具合的形態は図示のものに限られず、その全部または一部を、各種の負荷等に応じた任意の単位で、機能的または物理的に分散・統合して構成することができる。

【0114】例えば、各データベースを独立したデータベース装置として独立に構成してもよく、また、処理の一部をCGI(Common Gateway Interface)を用いて実現してもよい。

【0115】また、IPアドレス割当部302bをDHCPサーバ(図示せず)により実行してもよい。

【0116】また、情報端末装置200は、既知のパーソナルコンピュータ、ワークステーション、家庭用ゲーム装置、インターネットTV、情報家電装置、PHS端末、携帯電話端末、移動体通信端末またはPDA等の情報処理端末等の情報処理装置にプリンタやモニタやイメージスキャナ等の周辺装置を必要に応じて接続し、該情報処理装置にウェブ情報のブラウジング機能や電子メール機能を実現させるソフトウェア(プログラム、データ等を含む)を実装することにより実現してもよい。

【0117】この情報端末装置200の制御部は、その全部または任意の一部を、CPUおよび当該CPUにて解釈実行されるプログラムにて実現することができる。

すなわち、ROMまたはHDには、OS (Operating System) と協働してCPUに命令を与え、各種処理を行うためのコンピュータプログラムが記録されている。このコンピュータプログラムは、RAMにロードされることによって実行され、CPUと協働して制御部を構成する。

【0118】しかしながら、このコンピュータプログラムは、情報端末装置200に対して任意のネットワークを介して接続されたアプリケーションプログラムサーバに記録されてもよく、必要に応じてその全部または一部をダウンロードすることも可能である。あるいは、各制御部の全部または任意の一部を、ワイヤードロジック等によるハードウェアとして実現することも可能である。

【0119】また、本発明にかかるプログラムを、コンピュータ読み取り可能な記録媒体に格納することもできる。ここで、この「記録媒体」とは、フロッピー（登録商標）ディスク、光磁気ディスク、ROM、EPROM、EEPROM、CD-ROM、MO、DVD等の任意の「可搬用の物理媒体」や、各種コンピュータシステムに内蔵されるROM、RAM、HD等の任意の「固定用の物理媒体」、あるいは、LAN、WAN、インターネットに代表されるネットワークを介してプログラムを送信する場合の通信回線や搬送波のように、短期にプログラムを保持する「通信媒体」を含むものとする。

【0120】また、「プログラム」とは、任意の言語や記述方法にて記述されたデータ処理方法であり、ソースコードやバイナリコード等の形式を問わない。なお、「プログラム」は必ずしも単一的に構成されるものに限られず、複数のモジュールやライブラリとして分散構成されるものや、OS (Operating System) に代表される別個のプログラムと協働してその機能を達成するものをも含む。なお、実施の形態に示した各装置において記録媒体を読み取るための具体的な構成、読み取り手順、あるいは、読み取り後のインストール手順等については、周知の構成や手順を用いることができる。

【0121】また、ISP網600は、例えば、LAN（有線／無線の双方を含む）や、VANや、パソコン通信網や、公衆電話網（アナログ／デジタルの双方を含む）や、専用回線網（アナログ／デジタルの双方を含む）や、CATV網や、IMT2000方式、GSM方式またはPDC／PDC-P方式等の携帯回線交換網／携帯パケット交換網や、無線呼出網や、Bluetooth等の局所無線網や、PHS網や、CS、BSまたはISDB等の衛星通信網等のうちいずれかを含んでもよい。すなわち、本システムは、有線・無線を問わず任意のネットワークを介して、各種データを送受信することができる。

【0122】

【発明の効果】以上説明したように、この発明によれ

ば、ユーザが使用を許可するアプリケーションの種別に関するアプリケーション種別情報、および、ユーザが送受信を許可するデータの方角に関するデータ方向情報を登録し、ユーザに対してユーザIDおよびパスワードを発行し、ユーザが前記インターネットに接続する際に、ユーザの情報端末装置からユーザIDおよびパスワードを受信し、ユーザIDおよびパスワードがユーザに発行されたものであるか否かを認証し、認証された場合には、ユーザの情報端末装置に対してIPアドレスを割り当て、ユーザが送受信するデータが登録されたアプリケーション種別情報およびデータ方向情報に合致するか否かを判定し、合致すると判定されたデータについて送受信を許可するので、ユーザ個々にファイアウォール等の機材を導入することなく、セキュリティ知識のないユーザに対して安全なインターネット接続サービスを提供することができる。すなわち、ユーザは使用するアプリケーション種別とデータ方向をISP等に予め登録することにより、インターネットからユーザの情報端末装置への不正アクセスや、情報端末装置からインターネットへの不用意なデータ流出の可能性を低下させることができる。

【0123】つぎの発明によれば、ユーザがインターネットの接続を切断した場合には、IP割当手段によって割り当てた前記IPアドレスを無効にするので、ISP等に設定されたユーザの情報を削除することができるようになる。

【0124】つぎの発明によれば、登録されたアプリケーション種別情報および前記データ方向情報を変更するので、ユーザは、使用を許可するアプリケーションやデータ方向を随時変更することができるようになる。

【0125】つぎの発明によれば、条件判定によって合致しないと判定された場合には、データについて送受信するユーザの情報端末装置に対して警告メッセージを送信するので、拒絶されたアプリケーションやデータ方向等をユーザに通知することができるようになる。

【0126】つぎの発明によれば、ユーザが使用を拒絶するアプリケーションの種別に関する拒絶アプリケーション種別情報、および、ユーザが送受信を拒絶するデータの方角に関する拒絶データ方向情報をさらに登録し、ユーザが送受信するデータが登録された拒絶アプリケーション種別情報および拒絶データ方向情報に合致するか否かを判定し、条件判定によって拒絶アプリケーション種別情報および拒絶データ方向情報に合致すると判定した場合には、データを廃棄するので、ユーザは使用を拒絶するアプリケーションやデータの送受信を拒絶するデータ方向を予めISP等に登録することができるようになる。

【0127】つぎの発明によれば、登録されたアプリケーション種別情報と拒絶アプリケーション種別情報とを相互に変更可能にし、登録されたデータ方向情報と拒絶

10

20

30

40

50

データ方向情報とを相互に変更可能にするので、ユーザは、臨機応変に使用を許可または拒絶するアプリケーションやデータ方向を選択することができるようになる。

【0128】つぎの発明によれば、ユーザが使用を許可するアプリケーションの種別に関するアプリケーション種別情報、および、ユーザが送受信を許可するデータの方向に関するデータ方向情報を登録し、ユーザに対してユーザIDおよびパスワードを発行し、認証サーバにおいてユーザIDおよびパスワードが認証され、IPアドレスを割り当てられたユーザに対して、IPアドレスと、アプリケーション種別情報と、データ方向情報とを対応付けて格納し、格納されたIPアドレスと、アプリケーション種別情報と、データ方向情報とを中継装置に対して送信し、中継装置において、ユーザが送受信するデータがアプリケーション種別情報およびデータ方向情報に合致するか否かを判定し、合致すると判定されたデータについて送受信を許可するので、ユーザ個々にファイアウォール等の機材を導入することなく、セキュリティ知識のないユーザに対して安全なインターネット接続サービスを提供することができる。すなわち、ユーザは使用するアプリケーション種別とデータ方向をISP等に予め登録することにより、インターネットからユーザの情報端末装置への不正アクセスや、情報端末装置からインターネットへの不用意なデータ流出の可能性を低下させることができる。

【0129】つぎの発明によれば、ユーザがインターネットの接続を切断した場合には、IP割当手段によって割り当てた前記IPアドレスを無効にするので、ISP等に設定されたユーザの情報を削除することができるようになる。

【0130】つぎの発明によれば、登録されたアプリケーション種別情報および前記データ方向情報を変更するので、ユーザは、使用を許可するアプリケーションやデータ方向を随時変更することができるようになる。

【0131】つぎの発明によれば、ユーザが使用を拒絶するアプリケーションの種別に関する拒絶アプリケーション種別情報、および、ユーザが送受信を拒絶するデータの方向に関する拒絶データ方向情報をさらに登録し、ユーザが送受信するデータが登録された拒絶アプリケーション種別情報および拒絶データ方向情報に合致するか否かを判定し、条件判定によって拒絶アプリケーション種別情報および拒絶データ方向情報に合致すると判定した場合には、データを廃棄するので、ユーザは使用を拒絶するアプリケーションやデータの送受信を拒絶するデータ方向を予めISP等に登録することができるようになる。

【0132】つぎの発明によれば、登録されたアプリケーション種別情報と拒絶アプリケーション種別情報とを相互に変更可能にし、登録されたデータ方向情報と拒絶データ方向情報とを相互に変更可能にするので、ユーザ

は、臨機応変に使用を許可または拒絶するアプリケーションやデータ方向を選択することができるようになる。

【0133】つぎの発明によれば、ユーザが使用を許可するアプリケーションの種別に関するアプリケーション種別情報、および、ユーザが送受信を許可するデータの方向に関するデータ方向情報を登録し、ユーザに対してユーザIDおよびパスワードを発行し、ユーザが前記インターネットに接続する際に、ユーザの情報端末装置からユーザIDおよびパスワードを受信し、ユーザIDおよびパスワードがユーザに発行されたものであるか否かを認証し、認証された場合には、ユーザの情報端末装置に対してIPアドレスを割り当て、ユーザが送受信するデータが登録されたアプリケーション種別情報およびデータ方向情報に合致するか否かを判定し、合致すると判定されたデータについて送受信を許可するので、ユーザ個々にファイアウォール等の機材を導入することなく、セキュリティ知識のないユーザに対して安全なインターネット接続サービスを提供することができる。すなわち、ユーザは使用するアプリケーション種別とデータ方向をISP等に予め登録することにより、インターネットからユーザの情報端末装置への不正アクセスや、情報端末装置からインターネットへの不用意なデータ流出の可能性を低下させることができる。

【0134】つぎの発明によれば、ユーザがインターネットの接続を切断した場合には、IP割当工程によって割り当てた前記IPアドレスを無効にするので、ISP等に設定されたユーザの情報を削除することができるようになる。

【0135】つぎの発明によれば、登録されたアプリケーション種別情報および前記データ方向情報を変更するので、ユーザは、使用を許可するアプリケーションやデータ方向を随時変更することができるようになる。

【0136】つぎの発明によれば、条件判定によって合致しないと判定された場合には、データについて送受信するユーザの情報端末装置に対して警告メッセージを送信するので、拒絶されたアプリケーションやデータ方向等をユーザに通知することができるようになる。

【0137】つぎの発明によれば、ユーザが使用を拒絶するアプリケーションの種別に関する拒絶アプリケーション種別情報、および、ユーザが送受信を拒絶するデータの方向に関する拒絶データ方向情報をさらに登録し、ユーザが送受信するデータが登録された拒絶アプリケーション種別情報および拒絶データ方向情報に合致するか否かを判定し、条件判定によって拒絶アプリケーション種別情報および拒絶データ方向情報に合致すると判定した場合には、データを廃棄するので、ユーザは使用を拒絶するアプリケーションやデータの送受信を拒絶するデータ方向を予めISP等に登録することができるようになる。

【0138】つぎの発明によれば、登録されたアプリケ

10

20

30

40

50

ーション種別情報と拒絶アプリケーション種別情報とを相互に変更可能にし、登録されたデータ方向情報と拒絶データ方向情報とを相互に変更可能にするので、ユーザは、臨機応変に使用を許可または拒絶するアプリケーションやデータ方向を選択することができるようになる。

【0139】 つぎの発明によれば、上記の発明のいずれか一つに記載されたインターネット接続方法をコンピュータに実行させるプログラムとし、そのプログラムが機械読み取り可能となり、これによって、上記の発明のいずれか一つの動作をコンピュータによって実行することができるといふ効果を奏する。

【図面の簡単な説明】

【図1】 この発明の実施の形態1であるインターネット接続システムのネットワーク構成を示すブロック図である。

【図2】 本発明が適用される管理サーバ装置100の構成の一例を示すブロック図である。

【図3】 本発明が適用される認証サーバ装置300の構成の一例を示すブロック図である。

【図4】 本発明が適用される中継装置500の構成の一例を示すブロック図である。

【図5】 本発明が適用される情報端末装置200の構成の一例を示すブロック図である。

【図6】 本実施形態における本システムを用いて、ユーザがインターネットサービスを利用する際の動作の一例を示すフローチャートである。

【図7】 ユーザ情報データベース106aに格納されるユーザ情報の一例を示す図である。

【図8】 データ受信時の中継装置500の動作の一例を示すフローチャートである。

【図9】 実施の形態2である本システムの動作の一例

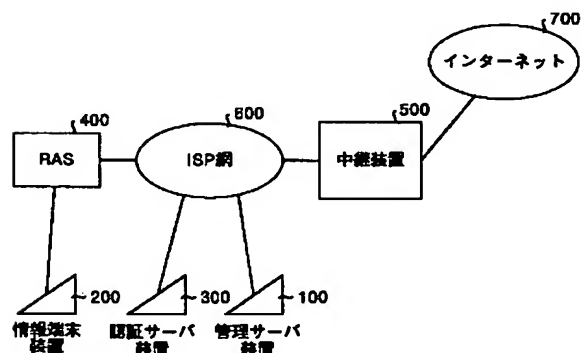
を示すフローチャートである。

【図10】 従来技術におけるファイアウォールが接続されたネットワーク構成図である。

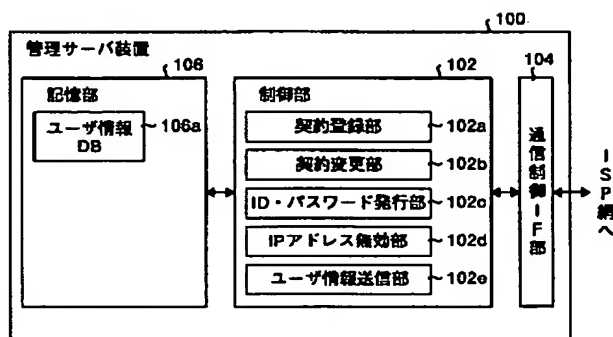
【符号の説明】

40 ユーザ名、41 割り当てIPアドレス、42 アプリケーション種別情報、43 データ方向情報、44 フラグ、60 組織内ネットワーク1、61 組織内ネットワーク2、62 組織内ネットワーク3、63 組織ネットワーク、64 ルータ、65 インターネット、66 ISP、67 端末、100 管理サーバ装置、102 記憶部、102a 契約登録部、102b 契約変更部、102c ID・パスワード発行部、102d IPアドレス無効部、102e ユーザ情報送信部、104 通信制御インターフェース部、106 記憶部、106a ユーザ情報データベース、200 情報端末装置、210 制御部、211 Webブラウザ、212 電子メール、220 ROM、230 HD、240 RAM、250 入力装置、260 出力装置、270 入出力制御インターフェース、280 通信制御インターフェース、300 認証サーバ装置、302 制御部、302a ユーザ認証部、302b IPアドレス割当部、304 通信制御インターフェース部、306 記憶部、306a ユーザ認証情報データベース、306b IPアドレス情報データベース、500 中継装置、502 制御部、502a データ受信部、502b ユーザ特定部、502c 条件判定部、502d データ送信部、502e 警告メッセージ送信部、502f ユーザ情報更新部、504 通信制御インターフェース部、506 記憶部、506a ユーザ情報データベース、600 ISP網、700 インターネット。

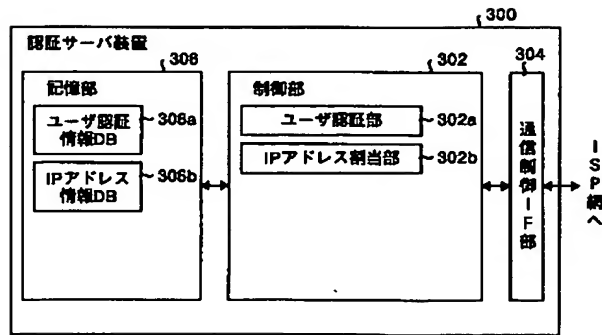
【図1】



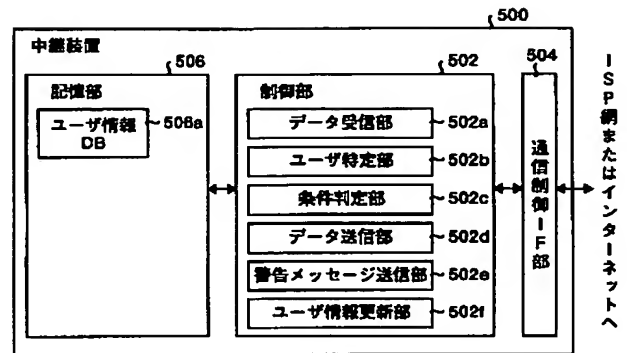
【図2】



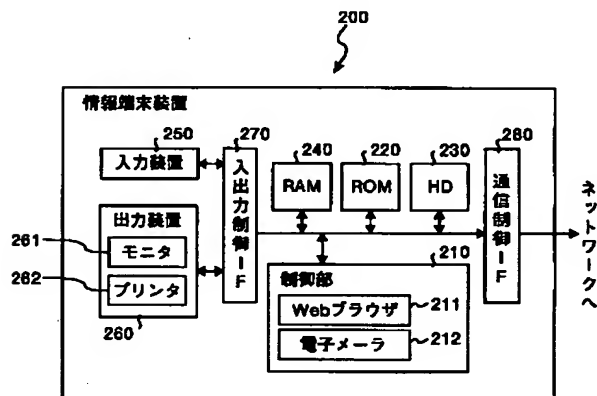
【図 3】



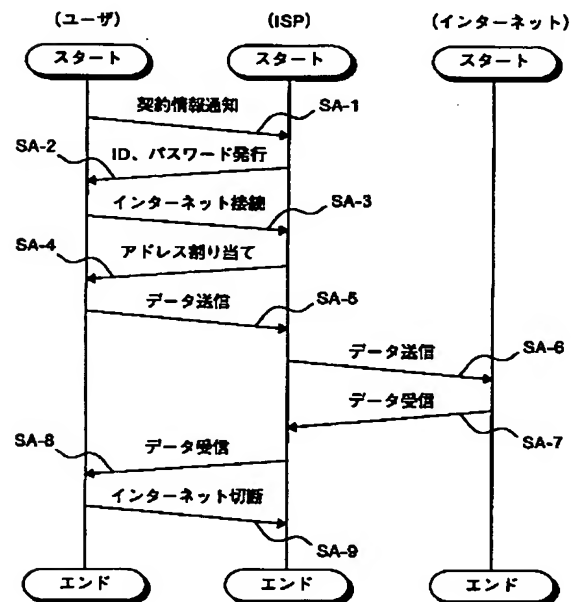
【図 4】



【図 5】



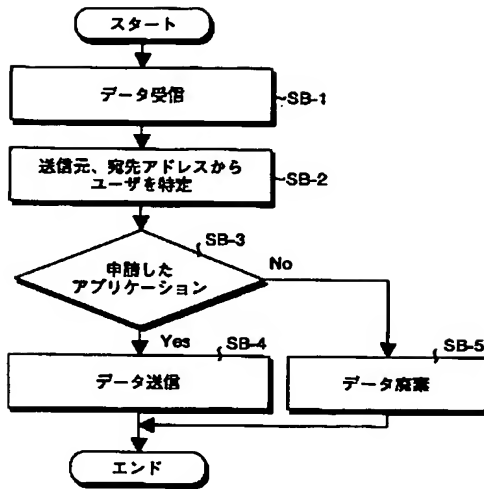
【図 6】



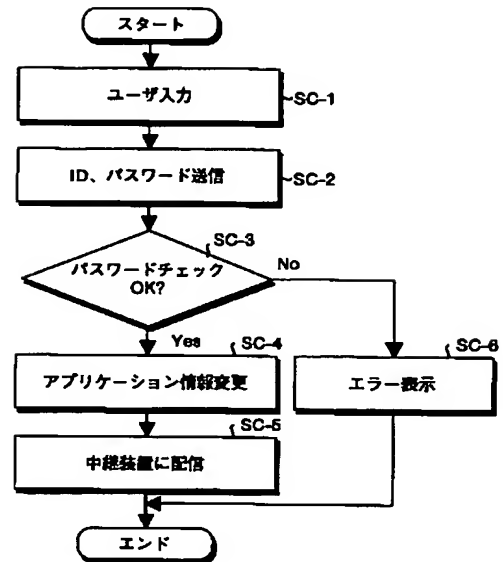
【図 7】

ユーザ名	割り当て IPアドレス	アプリケーション 種別情報	データ方向情報	許可/拒絶 を指定するフラグ
neko	192.168.0.100	E-mail	ユーザ>インターネット	許可
neko	192.168.0.100	www	ユーザ>インターネット	拒絶
⋮	⋮	⋮	⋮	⋮

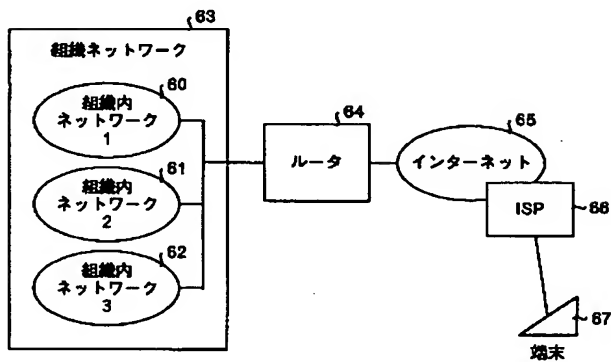
【図 8】



【図 9】



【図 10】



フロントページの続き

Fターム(参考) 5B085 AE01 AE23 BC00 BG07 CA04
 5B089 GA11 GA21 GB02 HA10 KA17
 5K030 GA15 HB16 HB21 HC01 HC14
 HD03 HD08 JA07 JA11 JL07
 JT03 JT06 KA06 KA07 KX24
 LB02 LC15 LC18 LD19 LD20
 MA04 MC08
 5K033 AA08 BA04 BA15 CA19 CB09
 CC02 DA05 DB14 DB18 DB20
 EA02 EA06 EC04